RESEARCH ARTICLE OPEN ACCESS

Cloud Computing Systems: Confidentiality Protection of Data

Mr. Chandan B [1], Mr. Vinay Kumar K [2]
Research Scholar [1]
Jain University, Bangalore
Manager [2]
IT& Smart Grid, BESCOM
Karnataka - India

ABSTRACT

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Cloud computing offers potential benefits including cost savings and improved business outcomes. However, there are a variety of information security risks that need to be carefully considered [5]. Risks will vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud vendor (also referred to as a cloud service provider) has implemented their specific cloud services. The Sensitive user data is unencrypted currently which is presented to remote third party service provider's machines, and there is high risk of utilisation of this sensitive information's. Currently there exists no effective way for protecting users' sensitive data from service providers in cloud computing [4]. In this paper, a methodology is presented to protect user's confidential data from service providers. As data owners no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the data for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission across the network [2]. We have two major approaches to ensure protection of user's confidential data namely Information hiding and Obfuscation of Data.

Keywords:- Data Confidentiality; Cloud Computing System Architecture; Data Obfuscation

I. INTRODUCTION

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet). Most importantly, this paper provides a list of thought provoking questions to help agencies understand the risks that need to be considered when using cloud computing.

Developing a risk assessment helps senior business representatives make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risk. Cloud computing as delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) [1] as " a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

II. USERS DATA CONFIDENTIALITY CONDITIONS

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or devices [3]. Hence, we must make sure that the users' Confidential data, which the users do not want to be accessed by service providers is not disclosed to service providers in the cloud computing systems, including applications, platforms, CPU and physical memories. It is noted that users' confidential data is disclosed to a service provider only if all of the following three conditions are satisfied simultaneously:

Condition 1: The service provider knows where the users' confidential data is located in the cloud computing systems.

Condition 2: The service provider has the privilege to access and collect the users' confidential data in the cloud computing systems.

Condition 3: The service provider can understand the meaning of the users' data. This is due to the following reasons: In order to collect users' data, the service provider must know the location of the data in cloud computing systems and have the privilege to access the data.

Even if the service provider can collect users' data successfully, the service provider may not be able to understand the meaning of the data unless the service provider has at the least some of the following information to understand the meanings of the data: i) types of data, ii) functionalities and interfaces of the application using the data and iii) format of the data Hence, if we can prevent the service providers from satisfying all the above three conditions, we can protect the confidentiality of users' data in cloud computing systems from the service providers.

III. FORMULATION OF PROBLEM STATEMENT

In Figure 1, Three different network entities can be identified as follows: Client : an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations; Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain clients' data; Third Party Auditor (TPA) [7] : a TPA, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

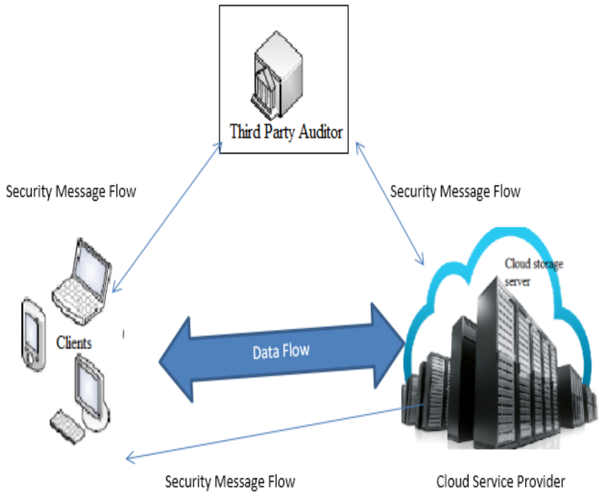


Fig 1: Cloud Entity Exchange Architecture

In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As clients no longer possess their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies [6] . In case that client does not necessarily have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA.

IV. EXISTING ARCHITECTURE

The current cloud computing system consists of three layers: software layer, platform layer and infrastructure layer, as shown in Figure 1. The software layer provides the interfaces for users to use service provider's applications running on a cloud infrastructure. The platform layer provides the operating environment for the software to run using system resources. The infrastructure layer provides the hardware resources for computing, storage, and networks. Platforms or infrastructures can be provided as virtual machines. Cloud computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unprecedented advantages in IT: on demand self-service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. One fundamental aspect of this new computing model is that data is being centralized or outsourced into the cloud. From the data owners' perspective, including both individuals and IT enterprises, storing data remotely in a cloud in a flexible on-demand manner brings appealing benefits: relief of the burden of storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, personnel maintenance, and so on.

V. ARCHITECTURE OF NEW APPROACH

The architecture consists of four different entities: data owner, user, Cloud Server (CS) and TPA. Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. Under the cloud paradigm, the data owner may represent either the individual or the enterprise customer, who relies on the cloud server for remote data storage and maintenance and thus is relieved of the burden of building and maintaining local storage infrastructure

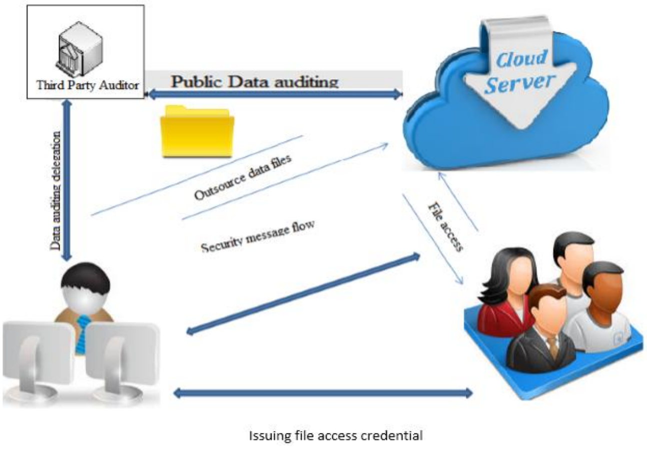


Fig 2: New Approach Architecture

Only the data owner can dynamically interact with the CS to update her stored data, while users just have the privilege of file reading. We focus on how to ensure publicly auditable secure cloud data storage services. As the data owner no longer possesses physical control of the data, it is of critical importance to allow the data owner to verify that his data is being correctly stored and maintained in the cloud. Considering the possibly large cost in terms of resources and expertise, the data owner may resort to a TPA for the data auditing task to ensure the storage security of her data, while hoping to keep the data private from the TPA. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the owners during the auditing process. The TPA should be able to efficiently audit the cloud data storage and without any additional Online burden for data owners.

VI. MODEL INETRACTIONS

The implementation part consists of four modules:

- Data owner module
- Cloud server module,
- TPA module
- User module.

A Data Owner Module

The data owner module is responsible for sending the data to the TPA and the Cloud server. Data owner sends the data like pdf, txt, htm, and html to the TPA. The TPA sends the message authentication code (MAC) and key by using SHA algorithm, to the owner. By using TPA, owner reduces his burden on worrying about the data. The owner sends that MAC and key to the user so that the user can access that data from the cloud server.

B. TPA Module

The TPA receives the data from the owner then sends the mac and key to the owner by using SHA algorithm. The TPA keeps monitoring the data in the cloud server. If data is deleted in the cloud server while trouble shooting or data may be deleted by the hacker. If the data is deleted then TPA automatically sends that backup data to the cloud server.

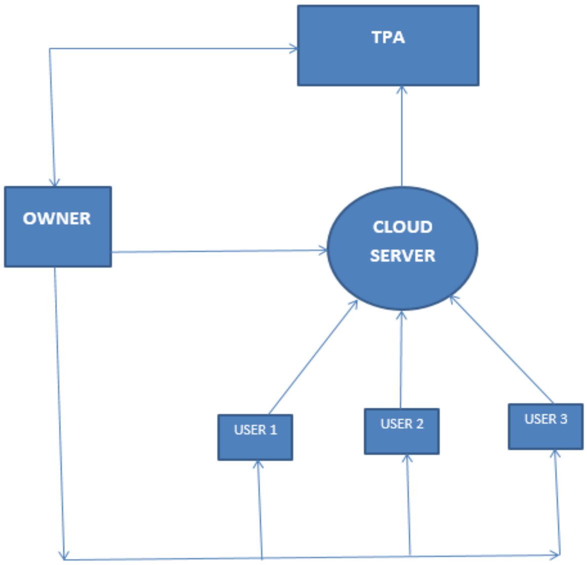
C. Cloud Server Module

In cloud server data is stored by the data owner. Cloud server is mainly responsible for storing the data from the owner.

Data in the server can be accessed by the user only when the user as data's mac and key.

D. User Module

If the user wants to access data from the cloud server then user needs to obtain the MAC and key from the data owner. Credentials will be given by owner to the user.



Owner sends data to cloud server. Owner gives permission to the users so that users can access the data from the cloud server. TPA keeps on monitoring the cloud server. While trouble shooting

Fig 3: Module Interaction Architecture

if the contents in the cloud server are damaged or corrupted then TPA send the data to the cloud server so that the user can access the data without any delay.

VII. DATA OBFUSCATION IN CLOUDS

Data obfuscation is the process of transforming the format or structure of data to hide the meaning of data. The major difference between encryption and obfuscation is that encrypted data cannot be processed until it is decrypted, but obfuscated data can be processed without de-obfuscation.

In our approach, data obfuscation is used to process users' data in an infrastructure cloud without revealing any users' specific confidential data to the infrastructure service providers. An approach to obfuscating data, which is transmitted from a user

to software layer of a cloud computing system for protecting user's privacy, is available [9], However, this approach is limited in the use of data obfuscation because the obfuscated data must fit into the user interfaces provided by service providers. In our approach, data obfuscation takes place between the software layer and the infrastructure layer

VIII. CONCLUSIONS

The TPA securely maintains the data in the cloud storage so that the user can access the data from anywhere. Following shows the interaction between 4 different entities. This Paper provides a list of thought provoking questions to help agencies understand the risks that need to be considered when using cloud computing [8]. Developing a risk assessment helps senior business representatives make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risk.
The questions in this Paper address the following topics:

1. Availability of data and business functionality
2. Protecting data from unauthorized access and
3. Handling security incidents

REFERENCES

[1] p. Mell and T.Grance, "Draft NIST working definition of cloud computing,"2009; http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[2] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," Univ.California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb. 2009.

[3] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," July 2008; http://status.aws.amazon.com/s3-20080720.html

[4] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," Dec. 2006; http://www.techcrunch.com/2006/12/28/gmail-disaster-reports-of-massemail-Deletions/

[5] M. Krigsman, "Apple's MobileMe Experiences Post-Launch Pain," July 2008;

[6] A. Juels, J. Burton, and S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM CCS '07, Oct. 2007, pp. 584–97.

[7] G.Ateniese et al., "Provable Data Possession at Untrusted Stores," Proc. ACM CCS '07, Oct. 2007, pp. 598–609.

[8] M. A. Shah et al., "Auditing to keep Online Storage Services Honest," Proc. USENIX HotOS'07, May 2007.

[9] G. Ateniese et al., "Scalable and Efficient Provable Data Possession," Proc. SecureComm '08, Sept. 2008.

[10] Con wang and kui Ren., "Toward publicly auditable secure cloud data storage services" August 2010

AUTHORS PROFILE

Vinay Kumar is completed his bachelors in Computer Science in VTU and Masters in Information Technology in Mysore University. He has an inter-disciplinary expertise benefit of being a IT Post graduate & having experience in Operations and Maintenance at BESCOM. His areas of interests are Smart Grid, CloudComputing, Scada &AMI.